IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Patent Application

Inventors: Sarvar PATEL

Docket No.:   2925-0161P

Lucent Case No.:   PATEL 7

Title: METHOD FOR TWO PARTY AUTHENTICATION AND KEY
                    AGREEMENT

ASSISTANT COMMISSIONER FOR PATENTS   Date: July 31, 1998
WASHINGTON, D.C. 20231

Sir:

Enclosed are the following papers relating to the above-named application for patent:

Specification
Formal Drawings (___2___ sheets)
Declaration and Power of Attorney
Assignment with Cover Letter

The fee has been calculated as shown below:

CLAIMS AS FILED				
	NO. FILED	NO. EXTRA	RATE	CALCULATIONS
Total Claims	22 - 20 =	2	x $22. =	$44.00
Independent Claims	2 - 3 =	0	x $82. =	-0-
Multiple Dependent Claim(s), if applicable			x $270. =	-0-
BASIC FEE				$790.00
			TOTAL FEE	$834.00

Please file the application and charge **Lucent Technologies Deposit Account No. 12-2325** the amount of $___834.00___, to cover the filing fee. Triplicate copies of this letter are enclosed. In the event of non-payment or improper payment of a required fee, the Commissioner is authorized to charge or to credit **Deposit Account No. 12-2325** as required to correct the error.
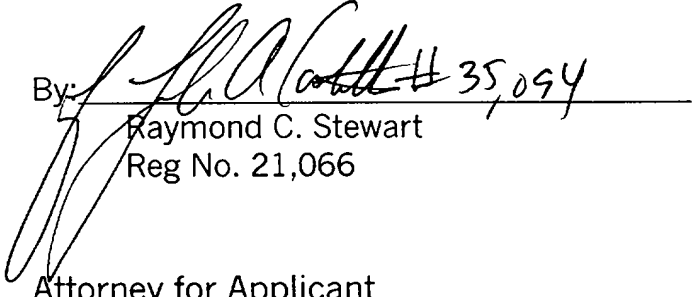
Please address all correspondence to:

BIRCH, STEWART, KOLASCH & BIRCH, LLP
P.O. Box 747
Falls Church, Virginia 22040-0747

Telephone inquiries may be directed to the undersigned representative at (703) 205-8000.

Respectfully submitted,

BIRCH, STEWART, KOLASCH & BIRCH, LLP

By: _____ 35,054

Raymond C. Stewart
Reg No. 21,066

RCS/GDY/jcp

Attorney for Applicant

METHOD FOR TWO PARTY AUTHENTICATION
AND KEY AGREEMENT

RELATED APPLICATIONS

The following applications, filed concurrently with the subject application, are related to the subject application and are hereby incorporated by reference in their entirety: application no. unknown entitled METHOD FOR UPDATING SECRET SHARED DATA IN A WIRELESS COMMUNICATION SYSTEM by the inventor of the subject application; application no. unknown entitled METHOD FOR TRANSFERRING SENSITIVE INFORMATION USING INTIALLY UNSECURED COMMUNICATION by the inventor of the subject application; application no. unknown entitled METHOD FOR SECURING OVER-THE-AIR COMMUNICATION IN A WIRELESS SYSTEM by the inventor of the subject application; and application no. unknown entitled METHOD FOR ESTABLISHING A KEY USING OVER-THE-AIR COMMUNICATION AND PASSWORD PROTOCOL AND PASSWORD PROTOCOL by the inventor of the subject application and Adam Berenzweig.

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to a method for authenticating parties communicating with one another, and in one application, a method for authenticating a mobile and a network in wireless communication. The present invention further relates to a key agreement based on the authentication protocol.

2. Description of Related Art

Protocols for authenticating parties communicating with one another provide a measure of security to the communication. Several such protocols are employed by the wireless industry and form part of the different communication standards in the U.S., Europe and Japan.

While the party authentication system and method according to the present invention is not limited to wireless communication, to promote ease of understanding, the present invention will described in the context of a wireless system. For this reason, a general overview of wireless systems is presented, including a discussion of the party authentication protocol used in at least one of the standards.

The U.S. currently utilizes three major wireless systems, with differing standards. The first system is a time division multiple access system (TDMA) and is governed by IS-136, the second system is a code division multiple access (CDMA) system governed by IS-95, and the third is the Advanced Mobile Phone System (AMPS). All three communication systems use the IS-41 standard for intersystem messaging, which defines the authentication

procedure for call origination, updating the secret shared data, and etc.

Fig.1 illustrates a wireless system including an authentication center (AC) and a home location register (HLR) 10, a visiting location register (VLR) 15, and a mobile 20. While more than one HLR may be associated with an AC, currently a one-to-one correspondence exists. Consequently, Fig. 1 illustrates the HLR and AC as a single entity, even though they are separate. Furthermore, for simplicity, the remainder of the specification will refer to the HLR and AC jointly as the AC/HLR. Also, the VLR sends information to one of a plurality of mobile switching centers (MSCs) associated therewith, and each MSC sends the information to one of a plurality of base stations (BSs) for transmission to the mobile. For simplicity, the VLR, MSCs and BSs will be referred to and illustrated as a VLR. Collectively, the ACs, HLRs, VLRs, MSCs, and BSs operated by a network provider are referred to as a network.

A root key, known as the A-key, is stored only in the AC/HLR 10 and the mobile 20. There is a secondary key, known as Shared Secret Data SSD, which is sent to the VLR 15 as the mobile roams (i.e., when the mobile is outside its home coverage area). SSD is generated from the A-key and a random seed RANDSSD using a cryptographic algorithm or function. A cryptographic function is a function which generates an output having a predetermined number of bits based on a range of possible inputs. A keyed cryptographic function (KCF) is a type of cryptographic function that operates based on a key; for instance, a cryptographic function which operates on two or more arguments (i.e., inputs) wherein one of the arguments is

the key. From the output and knowledge of the KCF in use, the inputs can not be determined unless the key is known. Encryption/decryption algorithms are types of cryptographic functions. So are one-way functions like
5   pseudo random functions (PRFs) and message authentication codes (MACs). The expression $KCF_{SK}(R_N')$ represents the KCF of the random number R_N' using the session key SK as the key. A session key is a key that lasts for a session, and a session is a period of time such as the length of a
10 call.

In the IS-41 protocol, the cryptographic function used is CAVE (Cellular Authentication and Voice Encryption). When the mobile 20 roams, the VLR 15 in that area sends an authentication request to the AC/HLR 10,
15 which responds by sending that mobile's SSD. Once the VLR 15 has the SSD, it can authenticate the mobile 20 independently of the AC/HLR 10. For security reasons, the SSD is periodically updated.

Fig. 2 illustrates the communication between the
20 AC/HLR 10, the VLR 15 and the mobile 20 to update the SSD. As discussed above, the AC/HLR 10 generates a random number seed RANDSSD, and using the CAVE algorithm generates a new SSD using the random number seed RANDSSD. The SSD is 128 bits long. The first 64 bits serve as a
25 first SSD, referred to as SSDA, and the second 64 bits serve as a second SSD, referred to as SSDB. As shown in Fig. 2, the AC/HLR 10 provides the VLR 15 with the new SSD and the RANDSSD. The VLR 15 then sends the RANDSSD to the mobile 20 along with a session request SR. The session
30 request SR instructs the mobile 20 to perform the SSD update protocol which is described in detail below. In response to receipt of the RANDSSD and the session request

SR, the mobile 20 uses the CAVE algorithm to generate the new SSD using the RANDSSD, and generates a random number R_M using a random number generator. The mobile sends the random number R_M to the VLR 15. The mobile 20 also

5   performs the CAVE algorithm on the random number R_M using the new SSDA as the key. This calculation is represented by $CAVE_{SSDA}(R_M)$.

One of the VLR 15 and the AC/HLR 10, also calculates $CAVE_{SSDA}(R_M)$, and sends the result to the mobile 20. The

10   mobile 20 authenticates the network if $CAVE_{SSDA}(R_M)$, which it calculated, matches that received from the network.

Next, and usually after receiving a signal from the mobile 20 indicating verification, the VLR 15 generates a random number R_N, and sends the random number R_N to the

15   mobile 20. Meanwhile, the VLR calculates $CAVE_{SSDA}(R_N)$. Upon receipt of R_N, the mobile 20 calculates $CAVE_{SSDA}(R_N)$, and sends the result to the VLR 15. The VLR 15 authenticates the mobile if $CAVE_{SSDA}(R_N)$, which it calculated, matches that received from the mobile 20. The random numbers R_M

20   and R_N are referred to as challenges, while $CAVE_{SSDA}(R_M)$ and $CAVE_{SSDA}(R_N)$ are referred to as challenge responses. Once the authentication is complete, the mobile 20 and the network generate session keys using SSDB.

In this protocol, the SSD is itself used to answer

25   the challenges from the mobile 20 and the network. This allows an attack when an old RANDSSD and SSD pair are revealed. Knowing this pair is enough to query the mobile 20, and answer its challenge. Thus an attacker can issue an SSD update to the mobile 20, and answer the

30   challenge from the mobile. Once the revealed SSD is accepted, and despite a secure session key agreement protocol (i.e., a protocol on communication between a

mobile and a network to establish a session key), the attacker can impersonate the network and place a call to the mobile 20 under fraudulent identities. For example, the impersonator can insert his own caller id or name and

5   pretend to be someone else. The attacker can pretend to be a credit card company, and ask to verify card number and pin. Or even use the telephone company name in the caller name field and ask to verify calling card numbers, etc.

SUMMARY OF THE INVENTION

10   In a two party authentication method according to the present invention a first party issues a random number as a first challenge, and a second party responds with a first challenge response. The first challenge

15   response is generated by performing a keyed cryptographic function (KCF) on the first challenge and a count value using a first key. The second party increments the count value upon receipt of the first challenge, and uses the count value as a second challenge. The first party

20   verifies the second party based on the first challenge and receipt of the second challenge and the first challenge response. After verification, the first party performs the KCF on the second challenge using the first key to generate a second challenge response. Based on the

25   second challenge and receipt of the second challenge response, the second party verifies the first party. Using the first and second challenges, an encryption key is generated by both parties. In this manner, a different key, the first key, from the encryption key is used in

30   answering challenges. The present invention has many applications including the wireless industry wherein the

first and second parties are a network and mobile, respectively.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will become more fully understood from the detailed description given below and the accompanying drawings which are given by way of illustration only, wherein like reference numerals designate corresponding parts in the various drawings, and wherein:

Fig. 1 is a block diagram illustrating the basic components of a wireless system;

Fig. 2 illustrates the communication between the authentication center/home location register, visiting location register, and the mobile to update the secret shared data according to the IS-41 standard; and

Fig. 3 illustrates the communication between the network and the mobile to authenticate these two parties according to one embodiment of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

As discussed above, while the party authentication system and method according to the present invention is not limited to wireless communication, to promote ease of understanding, the present invention will described in the context of a wireless system. More specifically, the method or protocol for two party authentication according to the present invention will be described as employed by the wireless system shown in Fig. 1.

In contrast to the method or protocol discussed above with respect to Figs. 1 and 2, in the method according to the present invention, the AC/HLR 10 and the

mobile 20 also generate another key, referred to as the M-key, based on the A-key. For example, the M-key is generated by applying a pseudo random function (PRF) indexed by the A-key on a value known to the network and the mobile 20. A practical PRF is the well-known Data Encryption Standard-Cipher Block Chaining (DES-CBC) algorithm from NIST (National Institute of Standards). In a preferred embodiment, DES-CBC, indexed by the 64-bit A-key on a known value, produces a 64-bit M-key.

Fig. 3 illustrates the communication between the network and the mobile 20 to authenticate these two parties according to one embodiment of the present invention. As shown, the VLR 15 acts as a conduit for communication between the AC/HLR 10 and the mobile 20. More specifically, the authentication protocol according to the present invention is performed between the AC and the mobile 20.

As shown, one party, the AC/HLR 10, generates and sends a random number R_N to the other party, the mobile 20. Typically, the AC/HLR 10, in addition to sending the random number R_N, sends a session request SR specifying the type of protocol to be performed. Protocol types include, for example, call origination, secret shared data (SSD) update, call termination, and mobile registration.

In response, the mobile 20 generates a count value C_M, and performs a KCF on the random number R_N, the count value C_M, Type data, and id data ID_M using the M-key as the key. This calculation is represented a $KCF_{M-Key}(Type, ID_M, C_M, R_N)$. Preferably, the KCF is a keyed message authentication code such as HMAC, but could be a PRF such as DES-CBC. The mobile 20 includes a counter which generates the count value C_M. The mobile 20 increments the count value C_M prior

to generating the challenge response (i.e., KCF_{M-Key}(Type, ID_M, C_M , R_N)) to each challenge from the network.

The Type data represents the type of protocol being performed. The id data indicates that the communication issued from the mobile. Usually, id data 1 indicates that the communication is from the network, and id data 0 indicates that the communication came from the mobile. For the purposes of discussion, however, the id data for the mobile 20 is shown as ID_M and the id data for the network is shown as ID_N. The system and method for two party authentication does not require the inclusion of the Type data when performing the KCF on the random number R_N and the count value C_M. The Type data and the specific id data have been included as part of the application of the two party authentication method and system to a wireless system.

The mobile 20 sends count value C_M and KCF_{M-Key}(Type, ID_M, C_M , R_N) to the network. Because the AC/HLR 10 initiated the current protocol including the two party authentication protocol according to the present invention, the AC/HLR 10 knows the Type data. Also, because communication from mobiles include the same id data, this value is known by the AC/HLR 10 as well. Accordingly, based on the received count value C_M, the AC/HLR 10 calculates KCF_{M-Key}(Type, ID_M, C_M , R_N) and determines whether this calculated value matches the version received from the mobile 20. If a match is found, the AC/HLR 10 authenticates the mobile 20.

Once the mobile 20 has been verified, the AC/HLR 10 calculates KCF_{M-Key}(Type, ID_N, C_M), and sends the calculated result to the mobile 20. The mobile 20, meanwhile, calculates KCF_{M-Key}(Type, ID_N, C_M) as well. The mobile 20

then verifies whether the calculated version of KCF_{M-Key}(Type, ID_N C_M) matches the version received from the AC/HLR 10. If a match is found, the mobile 20 authenticates the network.

5   Furthermore, after performing this two party authentication protocol, other keys can be generated. For instance, if the wireless system of Fig. 1 used this two party authentication protocol as part of the SSD update protocol, then, after the mobile 20 authenticates the

10   network, the mobile 20 and the AC/HLR 10 both have the random number R_N and the count value C_M. Both the mobile 20 and AC/HLR 10 generate the SSD as $PRF_{A-Key}(C_M, R_N)$; wherein the PRF is preferably the DES-CBC algorithm. Alternatively, in other protocols, this same technique is

15   used to generate other keys.

When applied to a wireless system, the mobile 20 needs to store the count value C_M in semi-permanent memory so that during power down, the count value C_M is not re-initialized. This way, repetition of a count value is

20   prevented; repetition of the count value permits an attacker to prevail in his attack. In a preferred embodiment, the count value is initialized using a random number and generated using a large bit counter such as a 64 or 75 bit counter. This provides security even when the

25   mobile 20 crashes and loses the stored count value. Even if an attacker can cause a mobile to crash at will, and assuming it takes at least a second to initiate a session, it will take, for example, a year before the attacker manages to have the mobile repeat a count value when a 75

30   bit counter is used.

As a further alternative, instead of a sending a unique random number R_N, the initiating party (e.g., the

network) issues a global random number. Namely, for each communication, the initiating party issues a different, unique random number R_N in the embodiment of Fig. 3. However, in this alternative embodiment, the initiating

5 party issues the same random number R_N for each communication.

In the protocol according to the present invention the key previously established between the parties (e.g., A-key or SSD) is not used to answer challenges, and thus

10 the network impersonation problem discussed with respect to IS41 is not possible. Furthermore, even if the M-key is revealed to an attacker, there is no direct way to obtain the A-key therefrom because a one-way function was used to generate the M-key. Because an attacker uses prior

15 challenges and challenge responses when mounting an attack, such an attack will fail if made on the protocol according to the present invention. The reason is that the attacker will be using a challenge response based on an old count value. Consequently, the network will not

20 verify the attacker. Further, keys generated after authentication as discussed above will be generated by the PRF of the new challenge using the A-key, and the attacker does not know the A-key.

The invention being thus described, it will be

25 obvious that the same may be varied in many ways. Such variations are not to be regarded as a departure from the spirit and scope of the invention, and all such modifications are intended to be included within the scope of the following claims.

WHAT IS CLAIMED

1   1. A method for authenticating a first party at a
2 second party, comprising:
3   (a) receiving a random number from said first party
4 as a first challenge;
5   (b) incrementing a count value in response to
6 receiving said first challenge;
7   (c) generating a first challenge response by
8 performing a keyed cryptographic function (KCF) on said
9 first challenge and said count value using a first key;
10   (d) transferring said count value, as a second
11 challenge, and said first challenge response to said
12 first party;
13   (e) receiving a second challenge response from said
14 first party, said second challenge response being a
15 result of performing said KCF on said second challenge
16 using said first key; and
17   (f) verifying said first party based on said second
18 challenge and said second challenge response.

1   2. The method of claim 1, prior to said step (c),
2 further comprising:
3   (g) generating said first key using a root key.

1   3. The method of claim 1, wherein said step (c)
2 generates said first challenge response by performing
3 said KCF on said first challenge, said count value, and
4 an identifier for said second party using said first key.

1   4. The method of claim 1, further comprising:

2   (g) establishing a second key based on said first

3   and second challenges.

1   5. The method of claim 1, wherein said step (a)

2   eceives a global challenge as said first challenge from

3   said first party.

1   6. The method of claim 1, wherein said first party

2   is a network of a wireless system and said second party

3   is a mobile.

1   7. The method of claim 6, wherein said step (c)

2   generates said first challenge response by performing

3   said KCF on said first challenge, said count value and

4   type data using said first key, said type data indicating

5   a type of protocol being performed by said network and

6   said mobile.

1   8. The method of claim 6, wherein said step (c)

2   generates said first challenge response by performing

3   said KCF on said first challenge, said count value, an

4   identifier for said mobile, and type data using said

5   first key, said type data indicating a type of protocol

6   being performed by said network and said mobile.

1   9. The method of claim 6, further comprising:

2   (g) establishing a second key based on said first

3   and second challenges.

1   10. The method of claim 9, wherein said second key

2   is one of secret shared data and a session key.

1   11. The method of claim 6, wherein said step (b)
2   increments said count value using a bit counter of
3   greater than 64 bits and which was initialized using a
4   random number.

1   12. A method for authenticating a first party at a
2   second party, comprising:
3   (a) outputting a random number as a first challenge;
4   (b) receiving a second challenge and a first
5   challenge response from said first party, said second
6   challenge being a count value, and said first challenge
7   response being a result of performing a keyed
8   cryptographic function (KCF) on said first challenge and
9   said count value using a first key; and
10   (e) verifying said first party based on said first
11   challenge, said second challenge, and said first
12   challenge response.

1   13. The method of claim 12, further comprising:
2   (f) establishing a second key based on said first
3   and second challenges.

1   14. The method of claim 12, wherein said step (a)
2   outputs said first challenge as a global challenge.

1   15. The method of claim 12, wherein said first party
2   is a mobile of a wireless system and said second party is
3   a network.

1   16. The method of claim 15, further comprising:

2   (f) establishing a second key based on said first

3 and second challenges.

1   17. The method of claim 16, wherein said second key

2 is one of secret shared data and a session key.

1   18. The method of claim 12, further comprising:

2   (f) generating a second challenge response by

3 performing said KCF on said second challenge using said

4 first key; and

5   (g) transferring said second challenge response to

6 said second party.

1   19. The method of claim 18, wherein said step (f)

2 generates said second challenge response by performing

3 said KCF on said second challenge and an identifier for

4 said second party using said first key.

1   20. The method of claim 18, wherein said first party

2 is a mobile of a wireless system and said second party is

3 a network.

1   21. The method of claim 20, wherein said step (f)

2 generates said second challenge response by performing

3 said KCF on said second challenge and type data using

4 said first key, said type data indicating a type of

5 protocol being performed by said network and said mobile.

1   22. The method of claim 20, wherein said step (f)
2 generates said second challenge response by performing
3 said KCF on said second challenge, an identifier for said
4 network, and type data using said first key, said type
5 data indicating a type of protocol being performed by
6 said   network   and   said   mobile.

ABSTRACT OF THE DISCLOSURE

According to the two party authentication method, a first party generates and transfers a random number to a second party as a first challenge. The second party

5 increments a count value in response to the first challenge, generates a first challenge response by performing a keyed cryptographic function (KCF) on the first challenge and the count value using a first key, and transfers the count value, as a second challenge, and

10 the first challenge response to the first party. The first party verifies the second party based on the first challenge, the second challenge and the first challenge response. The first party also generates a second challenge response by performing the KCF on the second

15 challenge using the first key, and transfers the second challenge response to the second party. The second party verifies the first party based on the second challenge and the second challenge response. For instance, the first and second parties can be a network and mobile,

20 respectively, in a wireless system. Also, based on the first and second challenges, both the first and second parties may generate another key.
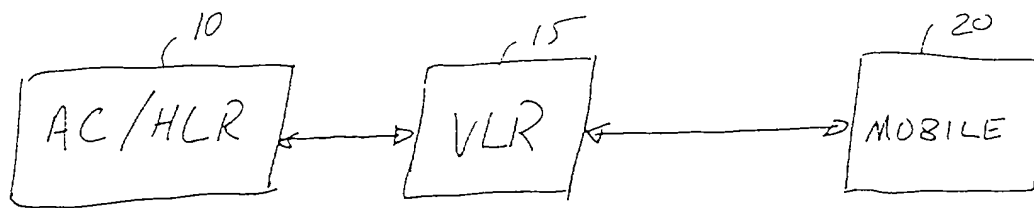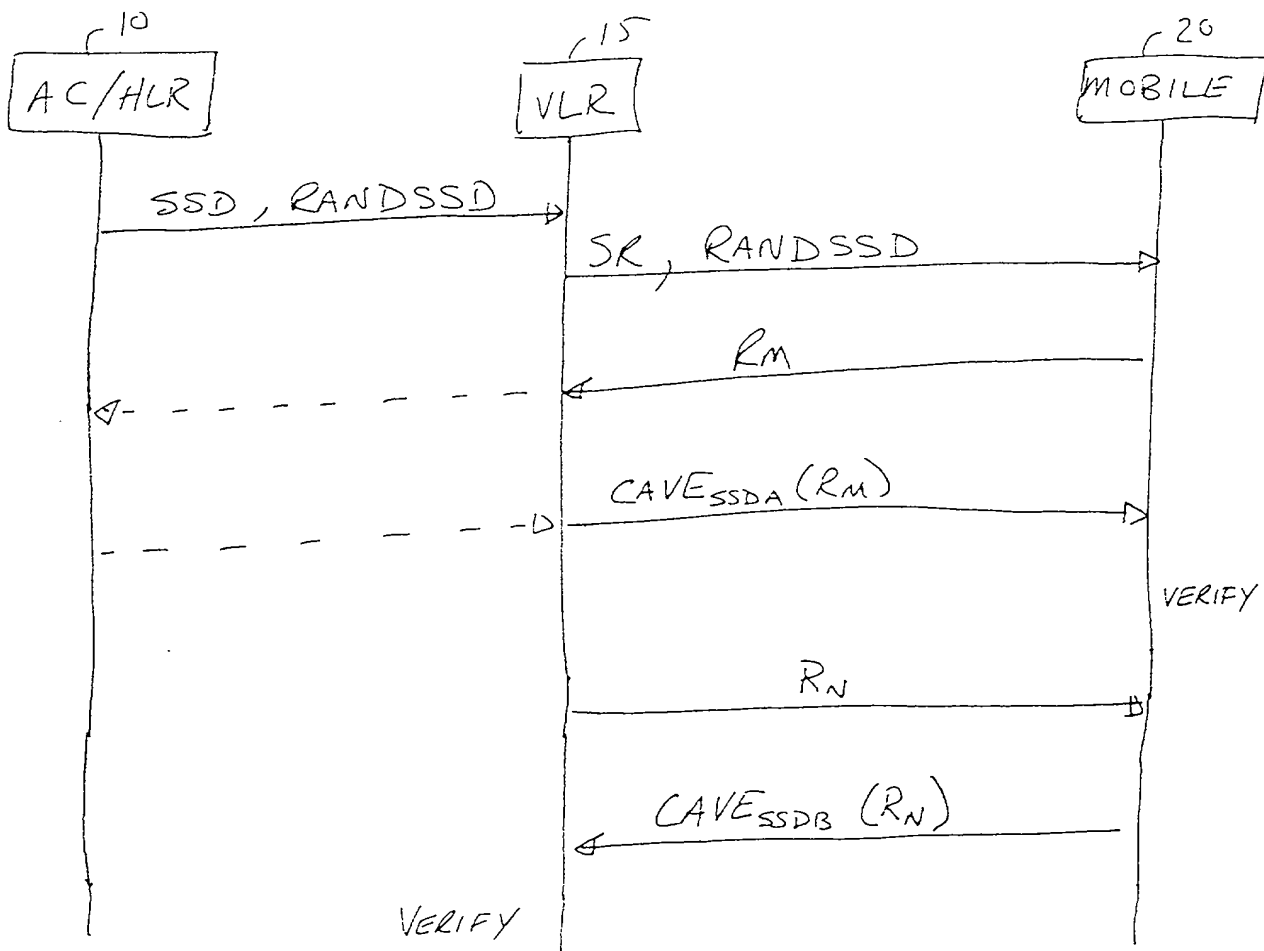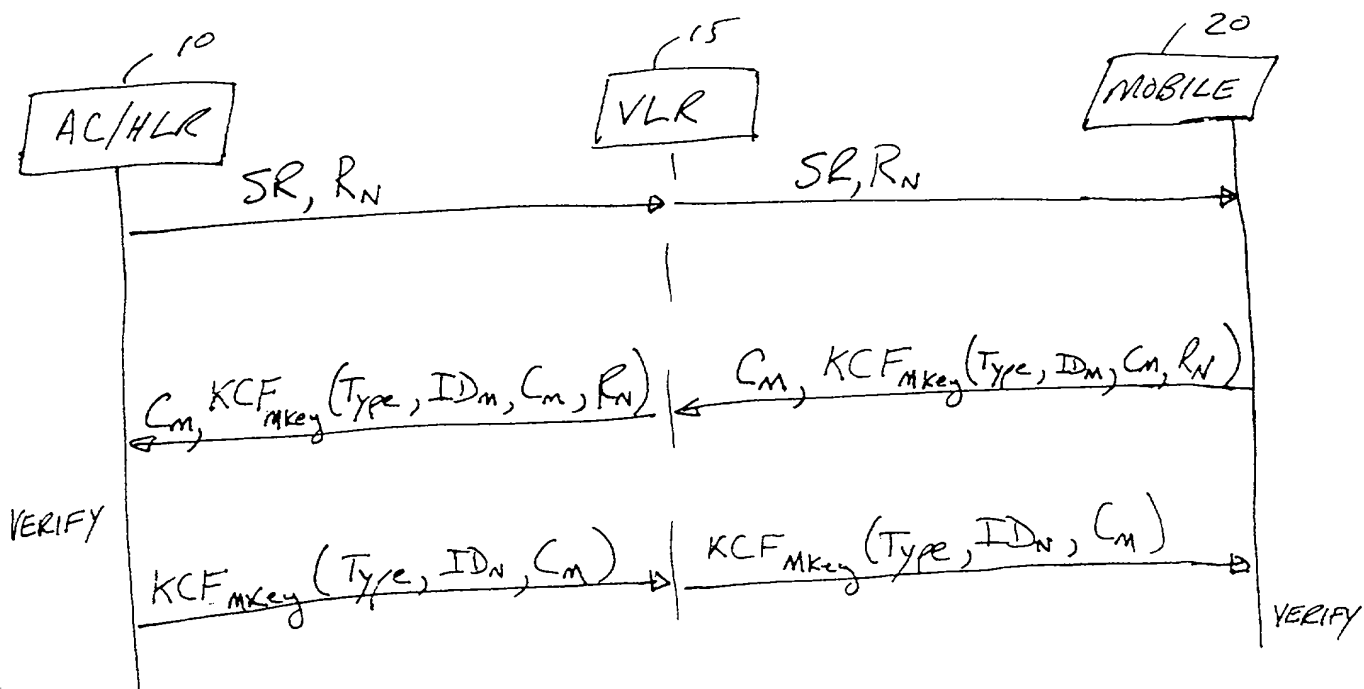
Fig. 1 Prior Art

Fig. 2 Prior Art

AC/HLR `10`   VLR `15`   MOBILE `20`

SR, R_N

SR, R_N

$C_M, KCF_{Mkey}(Type, ID_M, C_M, R_N)$

$C_M, KCF_{Mkey}(Type, ID_M, C_M, R_N)$

VERIFY

$KCF_{Mkey}(Type, ID_N, C_M)$

$KCF_{Mkey}(Type, ID_N, C_M)$

VERIFY

Fig. 3

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Declaration and Power of Attorney (sole inventor)

As the below named inventor I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor of the subject matter which is claimed and for which a patent is sought on the invention entitled METHOD FOR TWO PARTY AUTHENTICATION AND KEY AGREEMENT the specification of which is attached hereto or was filed on_____, as application Serial No. _____.

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment, if any, specifically referred to in this oath or declaration.

I acknowledge the duty to disclose all information known to me which is material to patentability as defined in Title 37, Code of Federal Regulations, § 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, § 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

None

I hereby claim the benefit under Title 35, United States Code, § 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, § 112. I acknowledge the duty to disclose all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, § 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application:

None

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

I hereby appoint the following attorney(s) with full power of substitution and revocation, to prosecute said application, to make alterations and amendments therein, to receive the patent, and to transact all business in the Patent and Trademark Office connected therewith:

Steven R. Bartholomew	(Reg. No. 34771)
Lester H. Birnbaum	(Reg. No. 25830)
Richard J. Botos	(Reg. No. 32016)
Jeffery J. Brosemer	(Reg. No. 36096)
Kenneth M. Brown	(Reg. No. 37590)
James A. DiGiorgio	(Reg. No. 36980)
Donald P. Dinella	(Reg. No. 39961)
Martin I. Finston	(Reg. No. 31613)
James H. Fox	(Reg. No. 29379)
Julio A. Garceran	(Reg. No. 37138)
Mony R. Ghose	(Reg. No. 38159)
Jimmy Goo	(Reg. No. 36528)
Anthony Grillo	(Reg. No. 36535)
John M. Harman	(Reg. No. 38173)
Donald E. Hayes Jr.	(Reg. No. 33245)
Michael B. Johannesen	(Reg. No. 35557)
Irena Lager	(Reg. No. 39260)
Frederick B. Luludis	(Reg. No. 26299)
Christopher N. Malvone	(Reg. No. 34866)
Scott W. McLellan	(Reg. No. 30776)
Geraldine Monteleone	(Reg. No. 40097)
John C. Moran	(Reg. No. 30782)
Michael A. Morra	(Reg. No. 28975)
Gregory J. Murgia	(Reg. No. 41209)
Claude R. Narcisse	(Reg. No. 38979)
Katharyn E. Olson	(Reg. No. 37693)
Joseph J. Opalach	(Reg. No. 36229)
Eugen E. Pacher	(Reg. No. 29964)
Jack R. Penrod	(Reg. No. 31864)
Daniel J. Piotrowski	(Reg. No. P-42079)
Gregory C. Ranieri	(Reg. No. 29695)
John T. Rehberg	(Reg. No. 29207)
Scott J. Rittman	(Reg. No. 39010)
Eugene J. Rosenthal	(Reg. No. 36658)
Bruce S. Schneider	(Reg. No. 27949)
Ronald D. Slusky	(Reg. No. 26585)
David L. Smith	(Reg. No. 30592)
Patricia A. Verlangieri	(Reg. No. P-42201)
John P. Veschi	(Reg. No. 39058)
David Volejnicek	(Reg. No. 29355)
Charles L. Warren	(Reg. No. 27407)
Eli Weiss	(Reg. No. 17765)

2

Please address all correspondence to BIRCH, STEWART, KOLASCH & BIRCH, LLP, P.O. Box 747, Falls Church, Virginia 22040-0747 (Mailing Address) or 8110 Gatehouse Road, Suite 500E, Falls Church, Virginia 22042 (Delivery Address). Telephone calls should be made to BIRCH, STEWART, KOLASCH & BIRCH, LLP by dialing (703) 205-8000, in the Washington, D.C. area.

Full name of sole inventor: _____Sarvar PATEL_____

By: _____   Date: __7/31/98__
        Inventor's signature

Residence:

_____Montville/Morris, NEW JERSEY_____
         City/County, State

Post Office Address:

_____34 Miller Lane, Montville, NEW JERSEY 07045__
         Street/P.O. Box, City, State, Zip

Citizenship: __USA_____

3